

WHAT IS CLAIMED IS:

1. A cable modem comprising:

5 a controller, monitoring incoming cable modem
transmissions for decryption keys, and monitoring
conditions when the decryption keys are received; and
a register, storing said decryption keys only when
said conditions meet the specified criteria.

10

2. A cable modem as in claim 1, wherein said cable
modem includes a key processing element which causes said
keys to be processed by software.

15

3. The cable modem as in claim 1, wherein said cable
modem is a host migrated cable modem in which a host PC
processes the keys.

20

4. A cable modem as in claim 1, wherein said register
includes a write enable function, which allows information
to be stored in said register only when said write enable
function is in a specified condition.

5. A cable modem as in claim 4, wherein said

controller allows operation with decryption keys only when said decryption keys are stored in said register.

6. A cable modem as in claim 1, wherein said register
5 includes a key destroy function, which allows a decryption key stored in said register to be marked as an invalid key, and prevents said key from being used for subsequent operations.

10 7. A cable modem as in claim 1, wherein said register stores a plurality of decryption keys, each decryption key being uniquely associated with a specified identification number indicative of services for which the decryption key is applicable.

15 8. A cable modem as in claim 1, wherein said register further includes a write enable function, associated with each identification number, and which enables keys to be stored in said register associated with said write enable
20 function only when said write enable function is in a specified state.

9. A method of controlling a cable modem, comprising:
monitoring an incoming cable stream for a decryption

key;

if a decryption key is present, then decrypting said decryption key in a host PC that is associated with the cable modem, but separate from the cable modem; and

5 allowing said decryption key to be used for decrypting said cable stream, only when said decryption key has been received in a specified way, otherwise not allowing said decryption key to be used for decrypting said cable stream.

10 10. A method as in claim 9 wherein said specified way includes that said decryption key was received over the cable medium.

15 11. A method as in claim 9, wherein said specified way includes that the decryption key was received associated with a particular service ID.

20 12. A method as in claim 9, wherein said specified way includes that the decryption key is stored in a specified register.

13. A method as in claim 9, further comprising storing the decryption key in a specified register when the allowing determines that said decryption key has been

received in the specified way.

14. A method as in claim 13, further comprising
allowing said decryption key to be used only when the
5 decryption key is stored in the register.

15. A method as in claim 9 wherein said specified way
includes requiring said decryption key to meet each of a
plurality of specified rules.

10

16. A method as in claim 15 wherein said specified
rules include key writing to a decryption engine being
normally disabled.

15

17. A method as in claim 15 wherein at least one of
said specified rules defines that the cable modem only
receives messages on the cable that are addressed to the
specified cable modem, and disregards messages which are
addressed to other than specified cable modem.

20

18. A method as in claim 15 wherein at least one of
the specified rules include that a specified service ID for
specified key ring material causes key write capability to
be enabled for said that specified service ID.

19. A method as in claim 18 further comprising an additional rule which disables key write for said service ID after key ring material is written to a storage area
5 associated with said service ID.

20. A method as in claim 18, further comprising an additional rule which disables key write for said service ID, for specified time after writing said key ring
10 material.

21. A method as in claim 15 wherein at least one of said specified rules include that the cable modem receives key ring material, writes said key ring material, and then
15 destroys said key ring material.

22. A system comprising:

a networked system of nodes, each said node being uniquely controlled according to a unique identifier;
20 at least one secure controller, said secure controller including a capability of providing permission to said nodes individually, according to said unique identifier;
wherein each said node includes a secure event detection element capable of receiving an encryption key

from said secure controller, and a memory, storing said encryption key only when specified conditions occur.

23. A system as in claim 22 where each said node is a
5 cable modem.

24. An article comprising a computer readable media,
comprising instructions causing the computer to:

monitor, in a first unit, a data stream for incoming
10 keys of a specified format;

send said keys to another unit, other than said first
unit, for decryption; and

enable use of said keys only when the keys are
received from the data stream in a specified way.

15

25. An article as in claim 24, wherein the stream is
a stream of cable modem information.

26. An article as in claim 25, wherein said keys are
20 DES encryption keys.

27. An article as in claim 24, further comprising
storing the keys in a specified location when they are
received in the specified way.

28. An article as in claim 27, wherein said keys are enabled for use only when they are stored in the specified location.

5

29. An article as in claim 28 further comprising instructions enabling writing only when specified conditions occur.

10

30. An article as in claim 28 further comprising instructions enabling specified keys to be destroyed.